ABSTRAK

UJI PENETRASI KEAMANAN SISTEM INFORMASI PADA *WEBSITE* MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)

(Studi Kasus Dinas Komunikasi dan Informatika Kabupaten Mesuji)

Oleh

AGHASTYA ICHSANUDIN ARIF

Keamanan website pada layanan digital pemerintah memiliki peran penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi publik. Penelitian ini bertujuan mengidentifikasi serta mengevaluasi kerentanan pada domain dan subdomain website Dinas Komunikasi dan Informatika Kabupaten Mesuji dengan menggunakan Penetration Testing Execution Standard (PTES). Kerangka PTES memberikan prosedur pengujian yang terstruktur, meliputi tahap intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, dan reporting. Beberapa alat seperti WhatWeb, Subfinder, Nmap, dan Xray digunakan untuk mengumpulkan informasi, melakukan enumerasi subdomain, memindai port terbuka, serta mendeteksi potensi celah keamanan. Hasil penelitian menunjukkan adanya sejumlah kerentanan dengan tingkat risiko beragam, termasuk konfigurasi server yang lemah, potensi SQL injection, penggunaan teknologi usang, serta paparan informasi sensitif. Pengujian eksploitasi memvalidasi bahwa beberapa kerentanan dapat dimanfaatkan untuk mengganggu keamanan sistem. Temuan ini menegaskan perlunya peningkatan praktik keamanan siber pada infrastruktur digital pemerintah. Rekomendasi mencakup penguatan konfigurasi server, pembaruan sistem berkala, penerapan mekanisme pertahanan berlapis, dan pelaksanaan uji penetrasi rutin untuk menjaga ketahanan sistem terhadap ancaman siber.

Kata kunci : uji penetrasi, analisis kerentanan, keamanan website, *SQL Injection*.

ABSTRACT

INFORMATION SYSTEM SECURITY PENETRATION TESTING ON WEBSITES USING THE PENETRATION TESTING EXECUTION STANDARD (PTES) METHOD

(Case Study of Dinas Komunikasi dan Informatika Kabupaten Mesuji)

By

AGHASTYA ICHSANUDIN ARIF

Website security in government digital services plays an important role in maintaining the confidentiality, integrity, and availability of public information. This study aims to identify and evaluate vulnerabilities in the domain and subdomain of the Mesuji Regency Communication and Information Agency website using the Penetration Testing Execution Standard (PTES). The PTES framework provides structured testing procedures, including intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting stages. Several tools such as WhatWeb, Subfinder, Nmap, and Xray were used to gather information, enumerate subdomains, scan open ports, and detect potential security gaps. The results of the study revealed a number of vulnerabilities with varying levels of risk, including weak server configuration, potential SQL injection, use of outdated technology, and exposure of sensitive information. Exploitation testing validated that some vulnerabilities could be exploited to compromise system security. These findings emphasize the need to improve cybersecurity practices in government digital infrastructure. Recommendations include strengthening server configurations, performing regular system updates, implementing layered defense mechanisms, and conducting routine penetration tests to maintain system resilience against cyber threats.

Keywords: penetration testing, vulnerability analysis, website security, SQL injection.